

Acceptable Use Policy

Author: Parke Hitchings



1 Overview

The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at Antonelli Institute in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

Antonelli Institute provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires the users of information assets to comply with company policies and protects the company against damaging legal issues.

2 Scope

All, students, at Antonelli Institute, must adhere to this policy. This policy applies to information assets owned or leased by Antonelli Institute, or to devices that connect to a Antonelli Institute network or reside at a Antonelli Institute site.

Information Security must approve exceptions to this policy in advance through a direct request of the administrator.

3 Policy Statement

3.1 General Requirements

- 3.1.1 You are responsible for exercising good judgment regarding appropriate use of Antonelli Institute resources in accordance with Antonelli Institute policies, standards, and guidelines. Antonelli Institute resources may not be used for any unlawful or prohibited purpose.
- 3.1.2 For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic per the Audit Policy. Devices that interfere with other devices or users on the Antonelli Institute network may be disconnected. Information Security prohibits actively blocking authorized audit scans. Firewalls and other blocking technologies must permit access to the scan sources.

3.2 System Accounts

- 3.2.1 You are responsible for the security of data, accounts, and systems under your control.

Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

- 3.2.2 You must maintain system-level and user-level passwords in accordance with the Password Policy.
- 3.2.3 You must ensure through legal or technical means that proprietary information remains within the control of Antonelli Institute at all times. Conducting Antonelli Institute business that results in the storage of proprietary information on personal or non-Antonelli Institute controlled environments, including devices maintained by a third party with whom Antonelli Institute does not have a contractual agreement, is prohibited. This specifically prohibits the use of an e-mail account that is not provided by Antonelli Institute, or its customer and partners, for company business.

3.3 Computing Assets

- 3.3.1 You are responsible for ensuring the protection of assigned Antonelli Institute assets that include the use of computer cable locks and other security devices. Laptops left at Antonelli Institute overnight must be properly secured or placed in a locked drawer or cabinet. Promptly report any theft of Antonelli Institute assets to the school store.
- 3.3.2 All PCs, PDAs, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set to 30 minutes or less. You must lock the screen or log off when the device is unattended.
- 3.3.3 Do not interfere with corporate device management or security system software, including, but not limited to, antivirus, Apple Remote Desktop, OS X firewalls, and device management or security software.

3.4 Network Use

You are responsible for the security and appropriate use of Antonelli Institute network resources under your control. Using Antonelli Institute resources for the following is strictly prohibited:

- 3.4.1 Causing a security breach to either Antonelli Institute or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniffing network traffic.
- 3.4.2 Causing a disruption of service to either Antonelli Institute or other network resources, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.
- 3.4.3 Introducing honeypots, honeynets, or similar technology on the Antonelli Institute network.
- 3.4.4 Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software.

- 3.4.5 Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws.
- 3.4.6 Use of the Internet or Antonelli Institute network that violates, Antonelli Institute policies, or local laws.
- 3.4.7 Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and keyloggers.
- 3.4.8 Port scanning or security scanning on a production network unless authorized in advance by Information Security.

3.5 Electronic Communications

The following are strictly prohibited:

- 3.5.1 Inappropriate use of communication vehicles and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates Antonelli Institute policies against harassment or the safeguarding of confidential or proprietary information.
- 3.5.2 Sending Spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication.
- 3.5.3 Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.
- 3.5.4 Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- 3.5.5 Use of an Antonelli Institute e-mail or IP address to engage in conduct that violates Antonelli Institute policies or guidelines. Posting to a public newsgroup, bulletin board, or listserv with an Antonelli Institute e-mail or IP address represents Antonelli Institute to the public; therefore, you must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the company.
- 3.5.6 Using Antonelli Institute computers or assets for commercial activities such as creating products or services for sale.

4 Enforcement

A student found to have violated this policy may be subject to disciplinary action, up to and including termination of enrollment.

5 Definitions

Term	Definition
honeypot, honeynet	Network decoys that serve to distract attackers from valuable machines on a network. The decoys provide an early warning for intrusion detection and detailed information on vulnerabilities.
Spam	Electronic junk mail or junk newsgroup postings. Messages that are unsolicited, unwanted, and irrelevant.



Terms of Service (TOS)

Please read the following information carefully before using the wireless high-speed internet access network. You may not use the service without accepting these Terms and Conditions.

Welcome to the wireless high-speed Internet access system ("Wi-Fi System") at ANTONELLI INSTITUTE. These "Terms and Conditions of Use", govern your rights and responsibilities and our rights and responsibilities relating to the use of the Wi-Fi System at ANTONELLI INSTITUTE.

Acceptance of Terms and Conditions of Use

BY SIGNING THE FILE DOCUMENTATION SHEET YOU ARE AGREEING that:

YOU HAVE READ, UNDERSTAND AND AGREE TO THE TERMS OF THIS AGREEMENT.

If you do not agree to the terms of this Agreement, you may not use the Wi-Fi System. Your acceptance of the Agreement by initialing the File Documentation Sheet has the same effect as if you had actually signed this Agreement. The effective date of this Agreement is the date that you initial the File Documentation Sheet.

Description of Wi-Fi System/Service Availability

ANTONELLI INSTITUTE will provide access to the Wi-Fi System at locations ("Enabled Locations") that have been equipped with wireless access points. Access points or Enabled Locations may not be available in all areas of the ANTONELLI INSTITUTE and may not always be operational.

ANTONELLI INSTITUTE will provide you with wireless card configuration support if needed.

Fee for Wi-Fi System

The Wi-Fi system at ANTONELLI INSTITUTE is provided "free of charge" as a value added service to the students, visitors, and business partners of ANTONELLI INSTITUTE.

Access to Internet

ANTONELLI INSTITUTE does not screen or restrict access to any content placed on or accessible through the Internet. ANTONELLI INSTITUTE also does not screen or restrict communications between parties via the Internet. You acknowledge that if you access the Internet you may receive or be exposed to content, goods, or services which you consider to be improper, inaccurate, misleading, defamatory, obscene, or otherwise offensive. You agree that ANTONELLI INSTITUTE is not liable for any action or inaction with respect to any such content on the Internet accessible through the Wi-Fi System.

Your Responsibilities

You must (1) provide all equipment (including computer hardware and software, personal digital assistants, wireless network cards, etc.) to connect to the Wi-Fi System, (2) comply with local, state, federal, and international laws and regulations, including but not limited to copyright and intellectual

property rights laws. You agree to be responsible for and to bear all risk and consequences for (1) the accuracy, completeness, reliability, and/or usefulness of any content available through the Wi-Fi System and (2) all communications that you send or receive via the Wi-Fi System. ANTONELLI INSTITUTE does not undertake the security of any data you send through the Wi-Fi System and it is your responsibility to secure such data.

Acceptable Use Policy

All users of the Wi-Fi System must comply with this Acceptable Use Policy (AUP). This AUP is intended to prevent unacceptable uses of the internet. ANTONELLI INSTITUTE does not actively monitor the use of the Wi-Fi System under normal circumstances. Similarly we do not exercise editorial control or review the content of any Web site, electronic mail transmission, newsgroup or other material created or accessible over or through the Wi-Fi System. However, we may review, monitor, remove, block, filter, or restrict by any other means any materials that, in our sole discretion, may be illegal, may subject ANTONELLI INSTITUTE to liability or may violate this AUP. ANTONELLI INSTITUTE may cooperate with legal authorities and/or third parties in the investigation of any suspected or alleged crime or civil wrong. Violation of the AUP or TOS may result in the suspension or termination of your access to the Wi-Fi System and/or suspension or termination from your program of study.

The following constitute examples of violations of this AUP.

You agree not to use the Wi-Fi System to:

- (1) Transmit any material (by uploading, posting, email, or otherwise) that is unlawful, threatening, abusive, harassing, tortious, defamatory, obscene, libelous, invasive of another's privacy, hateful, or racially, ethnically, or otherwise objectionable;
- (2) Harm, or attempt to harm, minors in any way;
- (3) Impersonate any person or entity or falsely state or otherwise misrepresent your affiliation with a person or entity; forge headers or otherwise manipulate identifiers in order to disguise the origin of any material transmitted through the Wi-Fi System;
- (4) Transmit any material (by uploading, posting, email, or otherwise) that you do not have a right to make available under any law or under contractual or fiduciary relationships (such as inside information, proprietary, and confidential information learned or disclosed as part of employment relationships or under non disclosure agreements);
- (5) Transmit any material (by uploading, posting, email, or otherwise) that infringes any patent, trademark, trade secret, copyright, or other proprietary rights of any party;
- (6) Transmit (by uploading, posting, email, or otherwise) any unsolicited or unauthorized advertising, promotional materials, "junk mail," "spam," "chain letters," "pyramid schemes," or any other form of solicitation;
- (7) Transmit any material (by uploading, posting, email, or otherwise) that contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment;
- (8) Interfere with or disrupt the Service or servers or networks connected to the Service, or disobey any requirements, procedures, policies or regulations of networks connected to the Service;

(9) Intentionally or unintentionally violate any applicable local, state, national or international law, or any regulations having the force of law;

(10) "Stalk" or otherwise harass another; or collect or store, or attempt to collect or store, personal data about third parties without their knowledge or consent;

(11) Resell the Wi-Fi System without ANTONELLI INSTITUTE's authorization;

(12) Use the Wi-Fi System for high volume data transfers, especially sustained high volume data transfers, hosting a web server, IRC server, or any other server.

You understand and agree that ANTONELLI INSTITUTE may disclose your communications and activities using the Wi-Fi System in response to lawful requests by governmental authorities, including Patriot Act requests, and judicial orders.

ANTONELLI INSTITUTE requests that anyone who believes that there is a violation of this AUP direct the information to it@antonelli.edu and include "WIFI" in the subject line. If available, please provide the following information: (1) the IP address used to commit the alleged violation; (2) the date and time of the alleged violation; (3) evidence of the alleged violation; and (4) your contact details including full name, email address, and telephone number. When reporting an issue regarding unsolicited email, please provide a copy of the email messages with full headers which typically provides all of the above data. Other situations will require different methods of providing the necessary information.

Termination

You agree that ANTONELLI INSTITUTE may terminate this Agreement and cancel your access to the Wi-Fi System at any time, without notice and for any reason including, but not limited to, violation of any of the terms and conditions of this Agreement, security or safety reasons, and/or using the Wi-Fi System to perform any illegal activity. You further agree that in the event of termination for any reason, ANTONELLI INSTITUTE will have no liability to you.

Notice of Problems or Complaints

If you experience a problem accessing or using the Wi-Fi System, report the problem by submitting a support issue on one of the computers or email support@antonelli.edu and include "WIFI" in the subject line.

Modifications

ANTONELLI INSTITUTE may, at its sole discretion, modify the terms and conditions of this Agreement, including the AUP, at any time. Such modifications shall be binding and effective upon posting on the <http://www.antonelli.org/forms> page. You agree to periodically review the Terms of Service and AUP on the <http://www.antonelli.org/forms> page to maintain awareness of any modifications. By continuing to use the Wi-Fi System after such postings, you accept and agree to any and all such modifications.

Indemnification

You shall defend, indemnify and hold ANTONELLI INSTITUTE and its corporate affiliates and their respective officers, directors, stockholders, employees, contractors, agents, successors, and assigns harmless from and against, and shall promptly reimburse them for any and all losses, claims,

damages, settlements, costs, and liabilities of any nature whatsoever (including reasonable attorneys' fees) to which any of them may become subject arising out of, based upon, as a result of, or in any way connected with, your use of the Wi-Fi System or any breach of this Agreement.

No Warranty

THE WI-FI SYSTEM IS PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS, WITHOUT WARRANTIES OF ANY KIND. ANTONELLI INSTITUTE DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED, ERROR-FREE, OR FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS. ANTONELLI INSTITUTE MAKES NO EXPRESS WARRANTIES AND THE USER WAIVES ALL IMPLIED WARRANTIES INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF TITLE, NON INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE REGARDING ANY MERCHANDISE, INFORMATION OR SERVICE PROVIDED THROUGH ANTONELLI INSTITUTE OR THE INTERNET GENERALLY. THE USER EXPRESSLY ACKNOWLEDGES THAT THERE ARE, AND ASSUMES ALL RESPONSIBILITY RELATED TO, THE SECURITY, PRIVACY AND CONFIDENTIALITY RISKS INHERENT IN WIRELESS COMMUNICATIONS AND TECHNOLOGY AND ANTONELLI INSTITUTE DOES NOT MAKE ANY ASSURANCES OR WARRANTIES RELATING TO SUCH RISKS. NO ADVICE OR INFORMATION GIVEN BY ANTONELLI INSTITUTE OR ITS REPRESENTATIVES SHALL CREATE A WARRANTY.

Limitation of Liability

ANTONELLI INSTITUTE, ITS EMPLOYEES, AGENTS, VENDORS, AND LICENSORS ARE NOT LIABLE FOR ANY COSTS OR DAMAGES ARISING, EITHER DIRECTLY OR INDIRECTLY, FROM YOUR USE OF THE WI-FI SYSTEM OR THE INTERNET, SPECIFICALLY INCLUDING ANY DIRECT, INDIRECT, INCIDENTAL, EXEMPLARY, MULTIPLE, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES.